UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/934,166	08/20/2001	Ian Rhodes	930.337USW1	8265

32294   7590   05/07/2004

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 05/07/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _20 August 2001_.

2a)☐ This action is **FINAL**.　　　2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-59_ is/are pending in the application.

　　4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-59_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _20 August 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

　　Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

　　Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

　　a)☒ All　b)☐ Some * c)☐ None of:

　　　1.☒ Certified copies of the priority documents have been received.

　　　2.☐ Certified copies of the priority documents have been received in Application No. _____.

　　　3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
　　　　application from the International Bureau (PCT Rule 17.2(a)).

　　* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
　　Paper No(s)/Mail Date _7_.

4)☐ Interview Summary (PTO-413)
　　Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2.   Claims 1-23 and 25-58 are rejected under 35 U.S.C. 102(b) as being anticipated by Jacobson (US 5,548, 649).

        a.   <u>Referring to claims 1, 27, 37:</u>

               i.   Jacobson teaches:

                      (1)   selectively routing a communication from the first end terminal to the second end terminal over said relatively insecure intermediate network by means of one or more network elements triggerable to selectively route said communication **[i.e., referring to Figure 1, the foregoing problems are solved by a network local security bridge and corresponding method for bridging a first side of a network and a second side of the network. The first side includes local secure zone host devices within a local secure zone established by the network local security bridge. The second side includes remote secure zone host devices within remote secure zones established by network remote security bridges, wherein the bridges route the data packet from one side of the network to another (column 1, lines 27-35)]**; and

                      (2)   encrypting said selectively routed communication by means of an encryption engine before it traverses said intermediate network, wherein said one or more network elements and said encryption engine are located substantially within said first secure network **[i.e., the data packet processor encrypts the data frame of the first side data packet when its source and destination addresses**

respectively specify one of the local secure zone host devices and one of the remote secure zone host devices (column 1, lines 47-51)].

      b.   *Referring to claim 2:*

          i.   Jacobson further teaches:

          (1)   wherein said one or more network elements comprises switch means provided with control means and storage means [i.e., referring to Figure 1, network security bridges (104-1, 104-3), that are switches for "providing with control means and storage means", includes first and second side interface controllers and routes data packet from one side to another (column 1, lines 35-36)].

      c.   *Referring to claims 3 and 4:*

          i.   Jacobson further teaches:

          (1)   wherein said storage means is operable to store routing information and security information [i.e., referring to Figure 1, the network local security bridge includes first and second side interface controllers and data packet processor for encrypting/decrypting data frame. The first side interface controller receives from the first side of the network a first side data packet and the second side interface controller receives from the second side of the network a second side data packet. The received first and second side data packets each contain a source address, a destination address, and a data frame (column 1, lines 35-43)].

      d.   *Referring to claims 5-7, 14-15, 28-35, 43-46:*

          i.   These claims have limitations that is similar to those of claims 2-4, thus they are rejected with the same rationale applied against claims 2-4 above.

      e.   *Referring to claim 8:*

          i.   Jacobson further teaches:

          (1)   identifying said predetermined communication by means of one or more of the following: originating subscriber characteristics; destination subscriber characteristics; destination subscriber characteristics; payload

characteristics; and network service characteristics [**i.e., in the network, normal data and bridge management communication is made between and among the hosts, bridges, and the gateway with ethernet data packets (wherein "originating subscriber characteristics; destination subscriber characteristics; destination subscriber characteristics; payload characteristics; and network service characteristics" are considered to include in these data packets). These data packets include an ethernet header and an ethernet data frame. The ethernet header includes an ethernet source address, an ethernet destination address, and an ethernet protocol identifier. The ethernet data frame includes an IP header and an IP data frame or portion. The IP header includes an IP source address, an IP destination address, and an IP protocol identifier. The IP data frame includes the data that is to be communicated (column 2, lines 57-67)**].

      f.   *Referring to claims 9 and 10:*

      i.   These claims have limitations that is similar to those of claim 8, thus they are rejected with the same rationale applied against claim 8 above.

      g.   *Referring to claims 11, 18-21, 25, 36, 48-52, 55, 57:*

      i.   These claims have limitations that is similar to those of claims 1 and 4, thus they are rejected with the same rationale applied against claims 1 and 4 above.

      h.   *Referring to claims 12 and 13:*

      i.   These claims have limitations that is similar to those of claims 3 and 4, thus they are rejected with the same rationale applied against claims 3 and 4 above.

      i.   *Referring to claim 16:*

      i.   Jacobson further teaches:

      (1)   wherein a service management access point is provided for accessing and changing information held in the storage means [**i.e., from the information provided by the commands, that is "for accessing and changing information held in the storage means", issued with the user terminal, the bridge manager determines that the user seeks to perform a bridge local install or view**

operation. **After determining this, the bridge manager determines whether the user is authorized to perform the bridge local install or view operation. This is done by comparing the user's i.d. and password for accessing local bridge 104-1 with those stored in the authorization table 244 and looking up the user's authorization level in the authorization table 244 (column 10, lines 19-28)].**

           j.   *Referring to claim 17:*

                i.   Jacobson further teaches:

                   (1)   wherein said security information comprises decryption information, the distribution of said decryption information being triggered according to a predetermined schedule **[i.e., the bridges 104-1 to 104-3 include encryption and decryption software and/or hardware so that normal data communication and bridge management communication between secure zones 108-1 to 108-3 is made by encrypting and decrypting the IP data frame in the transmitted or received data packet (column 3, lines 31-36)].**

           k.   *Referring to claim 22:*

                i.   Jacobson further teaches:

                   (1)   wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route operated by trusted network operators **[i.e., referring to Figure 1, encrypted data packets transmit through network security bridges, 104-1 to 104-3, which includes first and second side interface controllers and data packet processor for encrypting/decrypting data frame (column 3, lines 31-36)].**

           l.   *Referring to claim 23:*

                i.   Jacobson further teaches:

                   (1)   wherein security information is transferred to the one or more network elements located in the second secure network by means of a secure communication route over a relatively insecure intermediate network **[i.e., referring to Figure 1, encrypted data packets transmit between secure zone 108-1 to 108-3 through network security bridges, 104-1 to 104-3, and pass over the area that are**

not within a secure zone, which contains unsecure hosts, 102-8 to 102-10 (column 3, lines 50-67 through column 4, lines 1-7)].

     m.   *Referring to claims 26, 41, 42, 58:*

          i.   These claims have limitations that is similar to those of claim 11, thus they are rejected with the same rationale applied against claim 11 above.

     n.   *Referring to claims 38, 39:*

          i.   Jacobson further teaches:

          (1)   including decryption means located substantially within the second secure network; wherein said decryption means are provided at the second end terminal **[i.e., referring to Figure 1, the data packet processor, which includes in network security bridge, decrypts the data frame of the second side data packet when its source and destination addresses respectively specify one of the remote secure zone host devices and one of the local secure zone host devices (column 1, lines 55-59)].**

     o.   *Referring to claim 40:*

          i.   Jacobson further teaches:

          (1)   wherein said decryption means are provided at a node other than the second end terminal **[i.e., referring to Figure 1, network security bridges (104-1 to 104-3) includes data packet processors, these are "decryption", for decrypting the data frame. Jacobson discloses three different data packet processors as shown in Figure 1].**

     p.   *Referring to claim 47:*

          i.   This claim has limitations that is similar to those of claim 17, thus it is rejected with the same rationale applied against claim 17 above.

     q.   *Referring to claim 53:*

          i.   This claim has limitations that is similar to those of claim 22, thus it is rejected with the same rationale applied against claim 22 above.

     r.   *Referring to claim 54:*

          i.   This claim has limitations that is similar to those of claim 23, thus it is rejected with the same rationale applied against claim 23 above.

     s.   _Referring to claim 56:_

          i.   This claim has limitations that is similar to those of claims 1 and 26, thus it is rejected with the same rationale applied against claims 1 and 26 above.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4.   Claims 24 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jacobson, and further in view of Thomas (US 6,421, 339 B1).

     a.   _Referring to claims 24 and 59:_

          i.   Jacobson does not mention:

          (1)   provided to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network.

          ii.   Thomas teaches:

          (1)   allowing a H.323 compliant user to roam to another H.323 compliant network that is recognized by that users home gatekeeper. After arriving at the visited network, the roaming user registers with a visited gatekeeper. The visited gatekeeper authorizes the registration by determining the network of the roaming user and that a roaming agreement exists between the visited and home network **(column 6, lines 20-27).**

          iii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

          (1)   include such roaming agreement in Jacobson's network security bridging system to have a capability to call to a H.323 compliant data packet network **(column 6, lines 40-42 of Thomas).**

iv.   The ordinary skilled person would have been motivated to:

(1)   include such roaming agreement in Jacobson's network security bridging system for accommodating roaming endpoint users across H.323 compliant network domains **(column 1, lines 6-8 of Thomas).**

Conclusion

5.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a.   Wang (US 6, 614, 774 B1) discloses under roaming agreements, subscribers of a service provider that is a party to an agreement with other service providers can access networks of the other service providers in accordance with the terms of the agreement (column 1, lines 45-49).

b.   Gilbrech (US 6, 173, 399 B1) discloses protocols and architecture for secure virtual private networks. Intraenterprise data communications are supported in a secure manner over the Internet or other public network space with the implementation of secure virtual private networks. Members of a virtual private network group exchange data that may be compressed, encrypted and authenticated, if the exchange is between members of the group (see abstract).

c.   Rune (US 5, 850, 444) discloses a generic communications network provides an encrypted communications interface between service networks and their subscribers.   When communications are initiated between a subscribing communications terminal and the generic network, the terminal compares a stored network identifier associated with a stored public key, with a unique identifier broadcast by the generic network (see abstract).

d.   Johnston (US 6, 373, 946 B1) discloses a satellite mobile telecommunications system includes mobile terminals 2a, 2b which can communicate with one another using end-to end encryption and decryption techniques (see abstract).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
April 28, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100